Taustatietoa

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Saksa
www.pilz.com

Lokakuu 2025

Yritysten, koneiden ja tuotteiden suojaus

Safety ja Industrial Security - Kaikki yhdestä paikasta

Ostfildern, lokakuu 2025 - **Security-tapahtumat eivät enää vaikuta vain IT-järjestelmiin, vaan yhä useammin myös tuotantoympäristöön (OT). Industrial Security -tapahtumiksi lasketaan kohdennettujen hyökkäysten lisäksi myös tahattomat manipuloinnit. Tuotannossa Industrial Securityn tehtävä on varmistaa koneiden käytettävyys sekä tietojen ja prosessien koskemattomuus ja luotettavuus. Korkein suojaustavoite on kuitenkin toiminnallinen turvallisuus. Sillä jos yritykset eivät hallinnoi omia tietojaan, yritys ja sen työntekijöiden turvallisuus ovat vaarassa: ilman Securityä ei ole Safetyä, ja ilman Safetyä ei ole ihmisten suojausta!**

EU:ssa on tunnustettu kasvava uhkatilanne ja lainsäädäntöä on mukautettu sen mukaisesti: yritystasolla **NIS 2 -direktiivi** edellyttää toimenpiteitä, joilla varmistetaan korkea yhteinen kyberturvallisuuden taso unionissa esimerkiksi tietoturvallisuuden hallintajärjestelmän avulla.

EU:n koneasetuksessa 2023/1230 säädetään nyt koneiden ja järjestelmien suojaamisesta manipuloinnilta ja edellytetään Industrial Security -toimenpiteitä koneen toiminnalliseen turvallisuuteen vaikuttaville osille.

Kyberkestävyyssäädöksessä (Cyber Resilience Act, CRA) edellytetään Security-toimia tuotteille, joissa on digitaalisia elementtejä. Näitä ovat ohjausjärjestelmät, IO-järjestelmät ja muut koneissa käytettävät komponentit.

Yritykset, koneet ja tuotteet – koneiden valmistajat ja käyttäjät kohtaavat erilaisia haasteita ja erilaisia oikeudellisia vaatimuksia kaikilla tasoilla.

Huippuluokan turvallisuus

Riippumatta siitä, että lainsäädäntö tekee Industrial Securitystä pakollista, on monia hyviä syitä paneutua aiheeseen ja pyytää neuvoja jo varhaisessa vaiheessa. Vakiintuneet prosessit ja koneiden käyttötavat voivat edistää manipulointia, jos niitä ei tarkisteta säännöllisesti. Esimerkiksi koneiden pitkä käyttöikä tarkoittaa usein sitä, että niihin liittyvät järjestelmät vanhenevat eivätkä jossain vaiheessa enää täytä uusimpia turvallisuusstandardeja. Näissä järjestelmissä on Security-aukkoja, joita ei voida enää korjata, koska palveluntarjoaja ei enää toimita Security-päivityksiä. Haittaohjelmilta suojautumista ei useinkaan voida toteuttaa loppulaitteissa, koska osa niistä on liian vanhoja ja niiden suorituskyky kärsisi, mikä voi johtaa tuotannon keskeytymiseen.

Askel askeleelta kohti parempaa Industrial Securityä

Viime kädessä tavoitteena on varmistaa, että liiketoiminta säilyy suojattuna, mutta yritysten on voitettava useita haasteita tämän tavoitteen saavuttamiseksi. Nämä haasteet vaihtelevat sovellettavien oikeudellisten vaatimusten tunnistamisesta, järjestelmien haavoittuvuuksien tunnistamisesta ja poistamisesta, tietoisuuden lisäämisestä ja työntekijöiden kouluttamisesta aina valvonnan toteuttamiseen asti. Koska Security on niin sanottu "liikkuva maali", on myös tarpeen tarkistaa säännöllisesti koneiden Industrial Securityn tila. On tärkeää, että yrityksessä on selkeät vastuualueet ja järjestelmällinen lähestymistapa, joka sisältää tarvittavan asiantuntemuksen kehittämisen.

Automaatioyritys Pilz on mukautunut näihin vaatimuksiin ja luonut koneenrakentajille ja käyttäjille kansainvälisesti räätälöidyn palveluvalikoiman, joka kattaa kokonaisvaltaisesti kaikki ihmisen ja koneen suojeluun liittyvät näkökohdat. Pilzin asiantuntijat tuntevat ajankohtaiset oikeudelliset ja standardointivaatimukset ja ottavat ne huomioon neuvonnassaan. Koulutuskurssit täydentävät tarjontaa yritysten Security-tietämyksen lisäämiseksi tai päivittämiseksi. Käytännön toteutusta tukevat Pilzin tuoteratkaisut, kuten I.A.M.-valikoima (Identification and Access Management) Safetyn ja Industrial Securityn parantamiseksi.

Luo oikea perusta

Jotta kone- ja laitostekniikan asiantuntijat voivat varmistaa omien koneidensa Industrial Securityn, he tarvitsevat vankkaa perustietämystä erityisesti lainsäädännöstä ja sovellettavista standardeista. Pilzin asiantuntijat jakavat tätä asiantuntemusta ”Industrial Securityn perusteet” -koulutuksessa. Osallistujat oppivat ymmärtämään tietoturvauhkia, tutustuvat asianmukaisiin suojatoimenpiteisiin ja parhaisiin käytäntöihin kone- ja verkkoturvallisuuden alalla. Ensimmäistä kertaa Security-aiheeseen tutustuvat oppivat, millä toimenpiteillä he voivat suojata koneita tehokkaasti verkkohyökkäyksiltä ja manipuloinnilta tuotannon tasolla.

CESA - Certified Expert for Security in Automation on Pilzin kaksipäiväinen asiantuntijakurssi, joka antaa osallistujille syvällistä Security-tietämystä uusimpien standardien mukaisesti, erityisesti IEC 62443 -standardisarjan ("Teollisuuden tietoliikenneverkot - Verkkojen ja järjestelmien IT-turvallisuus") osalta. Lisäksi käsitellään käytännön toimenpiteitä riskien vähentämiseksi, kuten kulunvalvontaa, verkkoturvallisuuden parantamista teknisin keinoin sekä organisatorisia toimenpiteitä turvallisuusriskien vähentämiseksi.

Osallistujat oppivat soveltamaan standardia oikein ja osoittamaan, että heidän automaatiojärjestelmänsä täyttävät kyberturvallisuusvaatimukset. Tentin läpäistyään osallistujat saavat maailmanlaajuisesti tunnustetun TÜV NORDin sertifikaatin "CESA - Certified Expert for Security in Automation".

Teoreettisen tiedon soveltaminen käytäntöön

Teoreettisen perustan ja koulutuskurssien pohjalta seuraava askel Industrial Securityn vahvistamisessa on jäsenneltyjen, käytännönläheisten prosessien soveltaminen. Operatiivisen teknologian (OT) konsultointi mahdollistaa siirtymisen teoreettisesta perustasta toteutettavissa oleviin strategioihin. Industrial Security -palvelut tunnistavat vaiheittaisen lähestymistavan avulla monimutkaisten järjestelmien haavoittuvuudet ja kehittävät toimenpiteitä riskien minimoimiseksi. Tämä johtaa kokonaisvaltaiseen turvallisuuskäsitteeseen.

Neljä askelta kohti parempaa Industrial Securitya

OT-Security-prosessi koostuu neljästä vaiheesta: suojaustarveanalyysi, Industrial Security -riskinarviointi, Industrial Security -konsepti ja Industrial Security -järjestelmän todentaminen.

Suojaustarveanalyysin aikana yritys määrittää koneen tai järjestelmän yksittäisten "omaisuuserien" suojausvaatimukset ja niiden suojaustavoitteet. Toisessa vaiheessa, riskinarvioinnissa, tarkastellaan kaikkia riskejä ja niiden esiintymistodennäköisyyttä kunkin osa-alueen osalta järjestelmän koko elinkaaren aikana. Seuraavaksi luodaan yksityiskohtainen Industrial Security -konsepti, johon sisältyy strategioita ja toimenpiteitä hyökkäysten, manipuloinnin ja käyttövirheiden aiheuttamien riskien torjumiseksi ja lieventämiseksi. Järjestelmän jatkuvaa turvallista toimintaa varten luodaan myös

käytäntöjä, sääntöjä ja ohjeita. Viimeisessä vaiheessa, Industrial Security -järjestelmän varmentamisessa, tarkistetaan toteutettujen vastatoimien tehokkuus.

Koneen käytettävyyden varmistaminen

Industrial Security Services -prosessi auttaa lieventämään tai estämään verkkohyökkäyksiä. Myös tahattomat Security-loukkaukset vähenevät. Tämä puolestaan lisää koneiden käytettävyyttä, tuottaa kustannussäästöjä ja varmistaa viime kädessä taloudellisen tehokkuuden säilymisen.

Tämä lähestymistapa suojaa ensisijaisesti koneen äärellä olevia ihmisiä asianmukaisilla turvatoimilla. Koska Security-tapahtumasta voi tulla este Safety-toimenpiteille. Esimerkiksi koneiden edessä oleva valoverho varmistaa, ettei käyttäjä astu vaaravyöhykkeelle. Jos hyökkääjä pystyy kuitenkin vaikuttamaan vastaavaan ohjaukseen ja mekanismiin, valoverhon suojatoimintaa ei voida enää taata. Security suojaa Safetya!

Ratkaisun toteutuksen yhteydessä on järkevää tarkastella Safetya ja Securitya yhdessä. Sillä ilman Securitya ei ole Safetya ja ilman Safetya ei ole ihmisten suojelua.

Selkeästi säännelty: Kuka saa tehdä mitä koneella?

Koneen ja sen käyttäjien turvallisuus on kiinni ihmisten tai verkkojen pääsynvalvonnasta. Kulkuaukot on suojattava luvattomalta pääsyltä siten, että esimerkiksi koneen ollessa toiminnassa vaara-alueella ei ole henkilöitä. Sillä jopa järjestelmän hyvässä tarkoituksessa tapahtuvalla käytöllä tai huollolla - olipa se sitten paikan päällä tai verkon kautta - voi olla kohtalokkaita seurauksia.

Tärkeä tekijä on tunnistus ja pääsyoikeuksien hallinta (I.A.M.), jolla säännellään selkeästi valtuutuksia ja pääsyoikeuksia yrityksessä.

Tähän kuuluvat organisatoriset toimenpiteet ja eritelmät sekä asianmukaiset turvatoiminnot. Pilzin PITreaderin kaltainen kulunvalvontajärjestelmä on tähän oikea tuotekomponentti. Näin käyttäjät voivat täyttää työntekijöiden suojelua, vastuuta, maksimaalista tuottavuutta ja tietosuojaa koskevat vaatimukset.

Vain kokonaisvaltainen Securityn ja Safetyn tarkastelu takaa kattavan suojan ihmisille ja koneille. Se, haluaako yritys puuttua Securityyn ja kuinka perusteellisesti, ei ole enää yrityksen harkinnassa. Security on lakisääteinen vaatimus. Koneenrakennusteollisuudessa Industrial Security ei ole vain IT:n tehtävä, vaan olennainen osa suunnittelua ja rakentamista. Securityn toteuttaminen jälkikäteen on aikaa vievää ja merkitsee yleensä käyttäjäystävällisyyden, toiminnallisuuden ja tuottavuuden heikkenemistä.

((Merkkejä: 9 784)))

((Kasten:))

Yleiskatsaus Industrial Securityä koskevaan EU:n lainsäädäntöön:

Erityisesti Euroopassa lainsäätäjät vastaavat uhkatilanteeseen useilla laeilla. Tämä tarkoittaa, että Euroopassa on maailman tiukimmat säädökset. Koordinointi muiden maiden kanssa on kuitenkin jo käynnissä, ja niissäkin säädetään vastaavia lakeja. Industrial Securityn maailmanlaajuinen yhdenmukaistaminen on näin ollen odotettavissa.

NIS 2: Lisää velvoitteita yrityksille

Verkko- ja tietoturvadirektiivi (NIS) on Euroopan unionin direktiivi, jolla pyritään vahvistamaan kyberturvallisuutta. Direktiivi on ollut voimassa vuodesta 2016, ja sitä on tähän mennessä sovellettu kriittisen infrastruktuurin tarjoajiin, kuten energia-, liikenne-, pankki- ja rahoituspalvelut, terveydenhuolto, juomaveden toimitus ja jakelu sekä digitaalinen infrastruktuuri. Näiden alojen palveluntarjoajien oli toteutettava "asianmukaiset varotoimenpiteet" Securityn osalta ja raportoitava vakavista kyberturvallisuuteen liittyvistä vaaratilanteista. Uusi NIS 2 -direktiivi ((EU) 2022/2555 ... toimenpiteistä korkeatasoisen yhteisen kyberturvallisuuden varmistamiseksi koko unionissa) edellyttää, että tulevaisuudessa huomattavasti useammat yritykset toteuttavat kyberturvallisuusriskien hallintatoimenpiteitä. NIS 2:ssa laajennetaan aloja esimerkiksi valmistus- ja tuotantoteollisuuteen, mukaan lukien koneenrakennus ja sähkölaitteiden valmistajat.

Se edellyttää riskianalyysejä ja turvallisuuskonsepteja tietojärjestelmiä, toimitusketjun suojausta ja henkilöstön turvallisuutta varten. Se sisältää myös kulunvalvontaan ja järjestelmänhallintaan liittyviä käsitteitä sekä johdon pakollisen koulutuksen.

Euroopan parlamentti ja EU:n neuvosto hyväksyivät direktiivin vuoden 2022 lopussa. Kuten kaikki EU:n direktiivit, myös NIS 2 -direktiivi ei ole suoraan voimassa ja sitova yksittäisissä EU:n jäsenvaltioissa, vaan jäsenvaltioiden on saatettava se osaksi kansallista lainsäädäntöään. Yritysten olisi hyvä käsitellä NIS 2 mahdollisimman pian ja tehdä yritykselle kattava Security-arviointi. Tähän kuuluu esimerkiksi tietoturvallisuuden hallintajärjestelmän (ISMS) perustaminen. ISO 27001 -tietoturvastandardin mukainen sertifiointi on tässä yhteydessä hyödyllinen.

NIS 2 esim. tuulivoimaloissa: NIS 2:n myötä myös koneiden valmistajien, kuten sähköntuotantojärjestelmien (esim. tuulivoimaloiden) valmistajien, on tulevaisuudessa täytettävä vaatimukset. Tuulivoimalan valmistaja puolestaan tarvitsee automaatioratkaisuja, ohjaimia tai antureita. Tietyn koon ylittävät sähkökomponenttien valmistajat kuuluvat myös NIS 2:n piiriin. Koska NIS 2:ssa säädetään myös toimittajien huomioon ottamisesta, Pilzin kaltaisen yrityksen on myös huolehdittava turvallisista toimitusketjuista ja asetettava toimittajilleen vaatimuksia. NIS 2 kattaa siis koko toimitusketjun.

Uusi koneasetus: ei CE-merkintää ilman Securityä

Konedirektiivi 2006/42/EY on erityisen tärkeä koneiden toiminnallisen turvallisuuden kannalta.

Koneiden valmistajien on jo pitkään täytynyt suorittaa vastaava vaatimustenmukaisuuden arviointimenettely ja CE-merkintä, jotta ne voivat tuoda koneita Eurooppaan.

Kesäkuussa 2023 julkaistu koneasetus on päivitetty vastaamaan tekniikan nykytilaa. Koska kyseessä on asetus, sitä ei tarvitse ensin saattaa osaksi kansallista lainsäädäntöä. Koneiden valmistajilla on 20. tammikuuta 2027 asti aikaa siirtyä uusiin vaatimuksiin ja noudattaa niitä voimaantulopäivästä alkaen.

Koneasetus korvaa aiemman konedirektiivin, ja toisin kuin edeltäjänsä, kyberturvallisuus säädetään siinä pakolliseksi. Kun konedirektiivi käsitteli pelkästään Safetyä, asetukseen on sisällytetty Securityä koskeva suojelutavoite "Korruptiolta suojautuminen" kohtaan "Olennaiset terveys- ja turvallisuusvaatimukset": Koneen

turvallisuustoimintoja ei saa heikentää tahattomalla tai tahallisella väärentämisellä.

Tämä uusi tie CE-merkintään herättää koneiden valmistajissa ja käyttäjissä useita uusia kysymyksiä, sillä niiden on tarkistettava nykyisiä Safety- ja Security-konseptejaan.

Kyberkestävyyssäädös: turvallisuus koko tuotteen elinkaaren ajan

Yrityksen ja koneen tarkastelun lisäksi on ehdottoman välttämätöntä toteuttaa Security-toimia myös suoraan laitteissa (esimerkiksi ohjauksissa). Euroopan komissio esitti syyskuussa 2022 asetusluonnoksen, jonka tarkoituksena on lisätä tuotteiden kyberturvallisuutta. Tämä kyberturvallisuussäädös (CRA) on suunnattu sellaisten tuotteiden valmistajille, joissa on digitaalisia elementtejä (laitteistoja ja ohjelmistoja), eli itse asiassa lähes kaikille koneiden valmistajille. Tämä vaikuttaa sekä B2C-sektorin tuotteisiin, kuten älypuhelimiin tai robotti-imureihin, että B2B-sektorin tuotteisiin, kuten ohjausjärjestelmiin ja antureihin, sekä puhtaisiin ohjelmistotuotteisiin, kuten käyttöjärjestelmiin tai itse koneisiin.

Valmistajien velvollisuus ilmoittaa hyödynnetyistä haavoittuvuuksista tulee voimaan 11. syyskuuta 2026 alkaen. Digitaalisia elementtejä sisältävien tuotteiden on täytettävä CRA:n vaatimukset 11. joulukuuta 2027 alkaen, jotta ne voidaan asettaa saataville EU:n markkinoilla. Kyberkestävyyssäädös on EU:n asetus, joten sitä sovelletaan suoraan EU:n jäsenvaltioissa

Se, kuinka suuri vaikutus CRA:lla todellisuudessa on, riippuu siitä, mitä kriteerejä tuotteiden luokittelussa lopulta käytetään. Kyberkestävyyssäädöksen mukaan markkinoille saa nyt saattaa vain

tuotteita, joilla varmistetaan asianmukainen kyberturvallisuuden taso – tuotteen koko tuotteen elinkaaren ajan. Security alkaa siis tuotteen kehityksestä. Pilz on myös jo muutaman vuoden ajan yhdenmukaistanut kehitysprosessinsa standardin IEC 62443-4-1 "Teollisuusautomaation ohjausjärjestelmien turvallisuus - osa 4-1: Turvallisen tuotekehityksen elinkaarivaatimukset" kanssa ja kehittänyt esim. SecurityBridgen todistettavasti "turvallisesti".

((Merkki: 6 062)))

Pilz – The Spirit of Safety

Pilz on globaali automaatiotekniikan tuotteiden, järjestelmien ja palvelujen toimittaja. Turvallisen automaation pioneerina Pilz luo turvallisuutta ihmisille, koneille ja ympäristölle. Vuonna 1948 perustettu perheyritys, jonka pääkonttori sijaitsee Ostfildernissä, on nykyään maailmanlaajuisesti edustettuna 2 500 työntekijän voimin 42 tytäryhtiössä ja sivuliikkeessä.

Teknologiajohtaja tarjoaa täydellisiä automaatioratkaisuja koneen Safetyä ja Industrial Securityä varten. Tuotevalikoimamme sisältää anturi-, ohjaus- ja käyttötekniikan täydellisiä automaatioratkaisuja – mukaan luettuna järjestelmiä teollisuuden tiedonsiirtoon, diagnosointiin ja visualisointiin. Salkun täydentää kansainvälinen palvelutarjonta, johon sisältyy neuvonta, suunnittelu ja koulutus. Pilzin ratkaisuja käytetään kone- ja laitosrakentamisen lisäksi lukuisilla muilla aloilla, kuten intralogistiikassa, pakkaustekniikassa, rautatietekniikassa ja robotiikassa.

www.pilz.com

Pilz sosiaalisessa mediassa:

Sosiaalisen median kanavillamme kerromme taustatietoa Pilzistä ja yrityksessä työskentelevistä ihmisistä ja jaamme uutisia automaatiotekniikan alalta.

www.pilz.com/facebook
www.pilz.com/xing
www.pilz.com/youtube
www.pilz.com/linkedin

Yhteystiedot lehdistölle:

Martin Kurth
Yritys- ja ammattilehdistö
Puh: +49 711 3409-158

Sabine Karrer
Yritys- ja ammattilehdistö
Puh: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Jenny Skarman
Ammattilehdistö

Eva Gellner-Rössle
Ammattilehdistö

m.kurth@pilz.de

Puh: +49 711 3409-1067
j.skarman@pilz.de

Puh: +49 711 3409-7147
e.roessle@pilz.de